UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/620,156	07/14/2003	Seth Jerome Robertson	061164-0003US	9506

9629 7590 06/17/2009

MORGAN LEWIS & BOCKIUS LLP
1111 PENNSYLVANIA AVENUE NW
WASHINGTON, DC 20004

EXAMINER	
SIMITOSKI, MICHAEL J	
ART UNIT	PAPER NUMBER
2439	
MAIL DATE	DELIVERY MODE
06/17/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/620,156	ROBERTSON ET AL.	
	Examiner	Art Unit	
	MICHAEL J. SIMITOSKI	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 April 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *3,5-12 and 19-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *3,5-12 and 19-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 January 2008* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The response of 4/3/09 was received and considered.

2. Claims 3, 5-12 & 19-28 are pending.

Response to Arguments

3. Applicant's arguments with respect to claims 3, 5-12 & 19-28 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 3, 6-7, 9, 21-24 & 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 7,120,931 to Cheriton et al. (**Cheriton**) in view of U.S. Patent 6,279,113 to Vaidya et al. (**Vaidya**) and U.S. Patent Application Publication 2003/0196095 to Jeffries et al. (**Jeffries**).

Regarding claim 3, Cheriton discloses receiving a plurality of messages (data, col. 5, lines 26-27) from a data sensor (router, col. 5, lines 26-27) located at a network audit point (netflow directory, col. 5, lines 26-27), said data sensor sampling data packets on said computer communications network and outputting said messages (packets are received, col. 5, lines 42-43 and output, col. 6, lines 7-9), each of said messages (packet flows) describing an event occurring on said communications network (data entering router, i.e. communication traffic), processing said messages to form extrapolated connection sessions (categorized flows, col. 6, lines 25-26 & lines 37-44) from which to determine a connection source for each message (sort by source address, col. 7, lines 1-6) by clustering packets exchanged

between two addresses within a specified time period (classifying flows based on source and destination, col. 5, lines 61-65, col. 6, lines 10-20, lines 39-42 & lines 56-61) where the addresses are not predetermined (the netflow directory clusters packets having a common source/destination, defined as a flow, col. 5, lines 61-65), and detecting a surveillance probe by grouping said connection sessions into a plurality of groups of related connection source addresses (creating multiple aggregate filters, which yields groups, col. 7, lines 1-6 and 58-59), but lacks scoring each group based on at least a quantity of network attack destinations and generating an alert for each group whose score is greater than an empirically derived threshold. However, Vaidya teaches that a group of packets can be analyzed to recognize an attack by determining that the count of certain characteristics in the packet stream, such as an attempt to access a file, exceeds a threshold (col. 8, lines 16-39), where a notification can be sent to a reaction module (col. 8, lines 37-39). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Cheriton to detect a surveillance probe by scoring the groups of flows and generate an alert for each group whose score is greater than an empirically derived threshold. One of ordinary skill in the art would have been motivated to perform such a modification to detect a potential attack, as taught by Vaidya. As modified, Cheriton lacks scoring each group specifically based on at least a quantity of attack destinations. However, Jeffries teaches detecting the spread of malicious software (¶21) by counting references of destination addresses (¶¶13-16) and comparing the count to a threshold (¶16) to determine if a gateway may be receiving random addresses (which are associated with malicious software, ¶16). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Cheriton to score each grouping of filter results based on the quantity of attack destinations (destination addresses) and compare those values to a predetermined threshold. One of ordinary skill in the art would have been motivated to perform such a modification to detect the spread of malicious software, as taught by Jeffries.

Regarding claim 6, Cheriton, as modified above by Vaidya, teaches generating a profile of surveillance activity (counter, col. 8, lines 30-31), said profile of surveillance activity comprising one or more of the following: the number of attacks per unit time/the temporal frequency trends of individual attacker (Z trying to access A) (event occurring a threshold number of times within a predetermined time interval, Vaidya, col. 8, lines 16-21).

Regarding claim 7, Cheriton, as modified above by Vaidya, teaches processing one or more said detected surveillance probes to produce a detected surveillance scan (user Z making access request for file A, col. 8, lines 21-24), said processing of one or more said detected surveillance probes to produce a detected surveillance scan comprising one or more of the following: modeling and detecting surveillance scans performed by a particular source (user Z, col. 7, lines 36-39 & col. 8, lines 26-28) by identifying a source address (user Z) that generates more than a specified number of probes (threshold) within a specified time period (10 minutes, col. 8, lines 21-28).

Regarding claim 9, Cheriton, as modified above by Vaidya, teaches generating a profile of surveillance activity (counter, col. 8, lines 30-31), said profile of surveillance activity comprising one or more of the following: the number of attacks per unit time/the temporal frequency trends of individual attacker (Z trying to access A) (event occurring a threshold number of times within a predetermined time interval, col. 8, lines 16-21).

Regarding claim 21, Cheriton discloses limiting the number of analyzed flows by reporting only source addresses that have a particular characteristic (for instant, all with a source of 3.xxx.xxx.xxx, col. 7, lines 33-52) and since Cheriton groups packets into flows, Cheriton discloses limiting the number of analyzed flows by reporting only source address groups that have certain characteristics (a source address group being 3.xxx.xxx.xxx and 3.141.xxx.xxx, col. 7, lines 50-57), but lacks explicitly that the groups are reported based on a specified number of probes within a specified period of time. However, as described above with respect to claim 7, Vaidya teaches that a group of packets can be analyzed to recognize an

attack by determining that the count of certain characteristics in the packet stream, such as an attempt to access a file, exceeds a threshold (col. 8, lines 16-39) within a predetermined period of time (col. 8, lines 26-28), where a notification can be sent to a reaction module (col. 8, lines 37-39). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Cheriton's flow classification to limit flows (detected scans) by reporting only source addresses and groups of source addresses that perform more than a specified number of probes (access attempts) within a specified time. One of ordinary skill in the art would have been motivated to perform such a modification to detect a potential attack, as taught by Vaidya.

Regarding claim 22, Cheriton discloses a system comprising a data sensor (router, col. 5, lines 26-27) located at a network audit point (netflow directory, col. 5, lines 26-27) that samples data packets on said computer communications network and outputs said messages (packets are received, col. 5, lines 42-43 and output, col. 6, lines 7-9), each of said messages (packet flows) describing an event occurring on said communications network (data entering router, i.e. communication traffic) and a processor (netflow directory, col. 5, lines 26-27) that processes said messages to form extrapolated connection sessions (categorized flows, col. 6, lines 25-26 & lines 37-44) from said sampled data packets from which to determine a connection source for each message (grouping by source, col. 7, lines 1-6) by clustering packets exchanged between two addresses within a specified time period (classifying flows based on source and destination, col. 5, lines 61-65, col. 6, lines 10-20, lines 39-42 & lines 56-61) where the addresses are not predetermined (the netflow directory clusters packets having a common source/destination, defined as a flow, col. 5, lines 61-65), and that by groups said connection sessions into a plurality of groups (creating multiple aggregate filters, col. 7, lines 58-59) of related connection source addresses (creating multiple aggregate filters, which yields groups, col. 7, lines 1-6 and 58-59), but lacks scoring each group based on at least a quantity of attack destinations and generating an alert for each group whose score is greater than an empirically derived threshold. However, Vaidya teaches that a group of packets can be analyzed to

recognize an attack by determining that the count of certain characteristics in the packet stream, such as an attempt to access a file, exceeds a threshold (col. 8, lines 16-39), where a notification can be sent to a reaction module (col. 8, lines 37-39). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Cheriton to detect a surveillance probe by scoring the groups of flows and generate an alert for each group whose score is greater than an empirically derived threshold. One of ordinary skill in the art would have been motivated to perform such a modification to detect a potential attack, as taught by Vaidya. As modified, Cheriton lacks scoring each group specifically based on at least a quantity of attack destinations. However, Jeffries teaches detecting the spread of malicious software (¶21) by counting references of destination addresses (¶¶13-16) and comparing the count to a threshold (¶16) to determine if a gateway may be receiving random addresses (which are associated with malicious software, ¶16). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Cheriton to score each grouping of filter results based on the quantity of attack destinations (destination addresses) and compare those values to a predetermined threshold. One of ordinary skill in the art would have been motivated to perform such a modification to detect the spread of malicious software, as taught by Jeffries.

Regarding claim 23, Cheriton, as modified above by Vaidya, teaches generating a profile of surveillance activity (counter, col. 8, lines 30-31), said profile of surveillance activity comprising one or more of the following: the number of attacks per unit time/the temporal frequency trends of individual attacker (Z trying to access A) (event occurring a threshold number of times within a predetermined time interval, Vaidya, col. 8, lines 16-21).

Regarding claim 24, Cheriton, as modified above by Vaidya, teaches processing one or more said detected surveillance probes to produce a detected surveillance scan (user Z making access request for file A, col. 8, lines 21-24), said processing of one or more said detected surveillance probes to produce a detected surveillance scan comprising one or more of the following: modeling and detecting surveillance

scans performed by a particular source (user Z, col. 7, lines 36-39 & col. 8, lines 26-28) by identifying a source address (user Z) that generates more than a specified number of probes (threshold) within a specified time period (10 minutes, col. 8, lines 21-28).

Regarding claim 28, Cheriton discloses limiting the number of analyzed flows by reporting only source addresses that have a particular characteristic (for instant, all with a source of 3.xxx.xxx.xxx, col. 7, lines 33-52) and since Cheriton groups packets into flows, Cheriton discloses limiting the number of analyzed flows by reporting only source address groups that have certain characteristics (a source address group being 3.xxx.xxx.xxx and 3.141.xxx.xxx, col. 7, lines 50-57), but lacks explicitly that the groups are reported based on a specified number of probes within a specified period of time. However, as described above with respect to claim 7, Vaidya teaches that a group of packets can be analyzed to recognize an attack by determining that the count of certain characteristics in the packet stream, such as an attempt to access a file, exceeds a threshold (col. 8, lines 16-39) within a predetermined period of time (col. 8, lines 26-28), where a notification can be sent to a reaction module (col. 8, lines 37-39). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Cheriton's flow classification to limit flows (detected scans) by reporting only source addresses and groups of source addresses that perform more than a specified number of probes (access attempts) within a specified time. One of ordinary skill in the art would have been motivated to perform such a modification to detect a potential attack, as taught by Vaidya.

6. Claims 5 & 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Cheriton** and **Vaidya**, as applied to claims 3 & 7 above, in view of U.S. Patent Application Publication 2003/0188189 to Desai et al. **(Desai)**.

Regarding claim 5, Cheriton lacks controlling false positive detections versus false negative detections. However, Desai teaches an intrusion detection system that establishes an intrusion by

comparing various activities to thresholds and as such teaches that adjusting pre-tuned thresholds improves accuracy and reduces the number of false positives (¶60). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Cheriton (as modified above by Vaidya) to include a mechanism for adjusting the metrics used to determine intrusions (such as an intrusion rate of col. 8, lines 16-39). One of ordinary skill in the art would have been motivated to perform such a modification to reduce the number of false positives, as taught by Desai (¶60).

Regarding claim 8, Cheriton lacks controlling false positive detections versus false negative detections. However, Desai teaches an intrusion detection system that establishes an intrusion by comparing various activities to thresholds and as such teaches that adjusting pre-tuned thresholds improves accuracy and reduces the number of false positives (¶60). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Cheriton (as modified above by Vaidya) to include a mechanism for adjusting the metrics used to determine intrusions (such as an intrusion rate of col. 8, lines 16-39). One of ordinary skill in the art would have been motivated to perform such a modification to reduce the number of false positives, as taught by Desai (¶60).

7. Claims 10, 12 & 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Cheriton** and **Vaidya**, as applied to claims 7 & 24 above, in view of U.S. Patent 6,424,654 to **Daizo**.

Regarding claims 10 & 25, Cheriton discloses the grouping of scanning hosts comprising modeling and detecting scans distributed across a series of source addresses by grouping addresses, (col. 7, lines 44-57, where the detection causes filtering of traffic from an IP address range; upon further investigation, the IP address range can be limited to a more narrow range). This section also describes how the flow analyzer will cause filtering of all packets from, for example, an ISP suspected of hosting an

attacker and once the attacker is identified, only analyzing and filtering packets from the attacker. Cheriton lacks subtracting one address from another and placing the two addresses in the same group if the difference is less than a specified amount. However, Daizo teaches that a client can be limited to a single DHCP server because a DHCP server is known to give out a certain range of IP addresses (col. 5, lines 22-27). The client has a reference address and subtracts from the reference address received IP addresses from different DHCP servers; the address with the smallest distance from the reference is the correct DHCP server (col. 5, lines 27-45). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Cheriton, as modified by Vaidya, to perform the grouping of addresses by subtracting a received IP address from one IP addresses of detected potentially harmful traffic and if it is within a certain range (such as the range described in Cheriton, col. 7, lines 49-56), grouping two the together. One of ordinary skill in the art would have been motivated to perform such a modification to determine if an IP address is within a certain range and hence to detect and filter all potentially harmful traffic from an ISP using a simple arithmetic method, as taught by Daizo (col. 2, lines 57-59).

Regarding claim 12, Cheriton discloses generating a profile of surveillance activity (Vaidya's counter, col. 8, lines 30-31), said profile of surveillance activity comprising one or more of the following: the number of attacks per unit time/the temporal frequency trends of individual attacker (Z trying to access A) (event occurring a threshold number of times within a predetermined time interval, col. 8, lines 16-21).

8. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Cheriton**, **Vaidya** and **Daizo**, as applied to claim 10 above, in further view of **Desai**.

Regarding claim 11, Cheriton, as modified above, lacks controlling false positive detections versus false negative detections. However, Desai teaches an intrusion detection system that establishes an intrusion by comparing various activities to thresholds and as such teaches that adjusting pre-tuned thresholds improves accuracy and reduces the number of false positives (¶60). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Cheriton to include a mechanism for adjusting the metrics used to determine intrusions (such as an intrusion rate of col. 8, lines 16-39). One of ordinary skill in the art would have been motivated to perform such a modification to reduce the number of false positives, as taught by Desai (¶60).

9. Claims 19 & 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Cheriton** and **Vaidya**, as applied to claims 3 & 22 above, in view of U.S. Patent 6,453,345 to Trcka et al. (**Trcka**).

Regarding claims 19 & 26, Cheriton lacks wherein the step of processing said messages to form extrapolated connection sessions and detecting a surveillance probe further comprises at least one of the steps listed. However, Trcka teaches that it is beneficial to analyze incoming packets for invalid data (such as a non-existent LAN address, col. 15, lines 51-52) to determine if a packet should be further analyzed (col. 15, lines 37-39) by setting a flag (col. 15, lines 50-51), where the flag is analyzed to determine if the packet is recorded for processing (col. 15, lines 58-62). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Cheriton to identify packets that have a particular arrangement of flags set (flagged as GOOD or BAD). One of ordinary skill in the art would have been motivated to perform such a modification to determine if the packet should be further analyzed, as taught by Trcka.

10. Claims 20 & 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Cheriton** and **Vaidya**, as applied to claims 3 & 22 above, in view of U.S. Patent Application Publication 2002/0174362 to Ullmann et al. (**Ullmann**).

Regarding claims 20 & 27, Cheriton lacks the steps listed. However, Ullmann teaches that small packets are less efficiently stored throughout a network (¶15) and therefore if it useful to determine packets having a size smaller than a predetermined threshold so that an administrator can be alerted to the source of the small packets (¶18). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Cheriton to identify connections (flows) with packets whose payloads are smaller than a predetermined limit. One of ordinary skill in the art would have been motivated to perform such a modification to identify wasteful packets on a network, as taught by Ullmann.

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. The Malan et al. and Poletto et al. references are cited for teaching detecting SYN attacks.

b. The Lee et al. reference is cited for teaching detecting probe attacks by detecting multiple attack destinations for a single source.

12. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH

shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL J. SIMITOSKI whose telephone number is (571)272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571)272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

June 11, 2009
/Michael J Simitoski/
Primary Examiner, Art Unit 2439